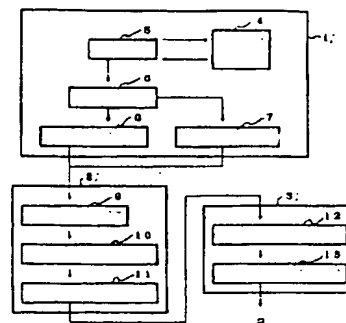


(54) APPLICATION PROGRAM END INFORMING SYSTEM

(11) 5-250325 (A) (43) 28.9.1993 (19) JP
 (21) Appl. No. 4-83116 (22) 5.3.1992
 (71) NEC CORP (72) HISAO YOSHIOKA
 (51) Int. Cl.⁵ G06F15/00, G06F13/00

PURPOSE: To accurately inform a terminal operator of the state at the end of an application program AP by an on-line system consisting of a host computer, a communication processor, and a terminal.

CONSTITUTION: In the on-line system wherein the terminal 3 and AP 4 have a communication through the communication processor 2 and host computer 1, it is checked whether or not the AP 4 ends normally or abnormally on the host computer 1 and if the AP 4 ends abnormally, AP end information including a classification and detailed information on the cause is sent to the communication processor 2. The communication processor 2 once receiving it generates a message to be sent to the terminal and sends it to the terminal 3, which displays the message on its display. Consequently, messages corresponding to all end states of the AP 4 are outputted, the terminal operator can easily grasp the reason of the end of the AP 4, and even if the AP ends abnormally, this system gives a system supervisor great effect to an easily fault analysis and remedy.



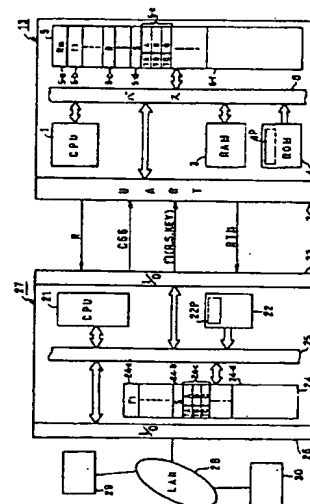
5: AP supervising means, 6: AP state control means, 7: AP normal end informing means, 8: AP fault information transmitting means, 9: AP end information receiving means, 10: AP end message generating means, 11: AP end message transmitting means, 12: AP end message receiving means, 13: AP end message display means, a: (displayed on a display unit, etc.)

(54) METHOD AND SYSTEM FOR AUTHENTICATION BETWEEN IC CARD AND TERMINAL MACHINE

(11) 5-250326 (A) (43) 28.9.1993 (19) JP
 (21) Appl. No. 4-49830 (22) 6.3.1992
 (71) MITSUBISHI ELECTRIC CORP (72) HISASHI OONO
 (51) Int. Cl.⁵ G06F15/00, G06F15/21, G06K17/00

PURPOSE: To improve the security by performing authentication operation between the IC card and terminal machine without directly transmitting any address.

CONSTITUTION: On the side of the IC card 13, a random number (R) is generated and sent to the side of the terminal machine 27. On the side of the terminal machine 27, authentication data f'1 (R, S, and KEY) ciphered according to a function of ciphering algorithm, e.g. ciphering algorithm F'1) are generated by utilizing a target authentication code (KEY) for the authentication and a system key (S) for ciphering and sent as data for the authentication back to the side of the IC card 13. On the side of the IC card 13, data f1 (R, S, KEY) ciphered according to a function of ciphering algorithm (f1) similar to the ciphering algorithm (f'1) of the terminal machine 27 are similarly generated by using the authentication code (KEY) stored in an area 5-e of an area 5-d and the system key (S) stored in an area 5-d by the IC card 3 itself and matched with the sent authentication data f'1 (R, S, and KEY).



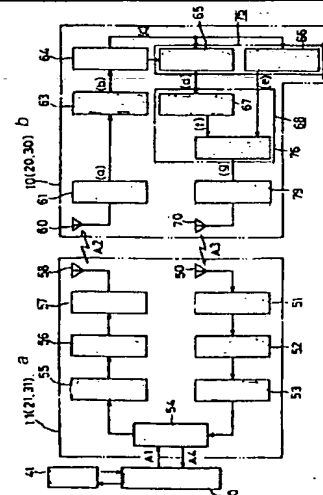
6: bus, 25: bus, 29 & 30: host computer, 5-f: data area, 24-d: work area and data area

(54) METHOD FOR DRIVING CIRCUIT IN SLEEPING MODE

(11) 5-250327 (A) (43) 28.9.1993 (19) JP
 (21) Appl. No. 4-84885 (22) 6.3.1992
 (71) SMK CORP (72) KATSUMI SAKAI(1)
 (51) Int. Cl.⁵ G06F15/00, H04B5/00

PURPOSE: To put only necessary irreducible internal circuits of the circuit in sleeping mode in operation and to put all the circuits in operation for the 1st time when an operation mode signal is detected.

CONSTITUTION: The circuit 10 in the sleeping mode employs the driving method which drives a circuit for sending a characteristic identification code with the reception output generated when a request-to-send signal which is higher than a constant reception level is received from a fixed station 11. The fixed station 11 repeatedly sends the request-to-send signal. In the circuit 10 in the sleeping mode, on the other hand, only the part of a signal detecting circuit 63 is in operation and detects whether or not there is the request-to-send signal. When the reception level is larger than the constant level, a mode switching control signal is outputted and all the circuits operate for the 1st time. The mode switching control signal is supplied as circuit driving electric power to the circuit 10 in the sleeping mode.



40: fixed station centralized control circuit, 41: control circuit, 51: tuning circuit, 52: amplifying circuit, 53: waveform shaping circuit, 54: microcomputer, 55: request-to-send signal generating circuit, 56: modulating circuit, 57: amplifying circuit, 61: tuning circuit, 64: timer circuit, 65: 1st clock generating circuit, 66: 2nd clock generating circuit, 67: identification code generating circuit, 68: modulating circuit, 75: clock generating circuit, 76: AND circuit, 79: transmitting circuit, a: fixed station, b: mobile station

Best Available Copy

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-250326

(43)公開日 平成5年(1993)9月28日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 G	7459-5L		
15/21	3 4 0 C	7218-5L		
G 0 6 K 17/00	D	7459-5L		
	T	7459-5L		

審査請求 未請求 請求項の数15(全 23 頁)

(21)出願番号 特願平4-49830

(22)出願日 平成4年(1992)3月6日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 大野 久支

伊丹市瑞原4丁目1番地 三菱電機株式会
社北伊丹製作所内

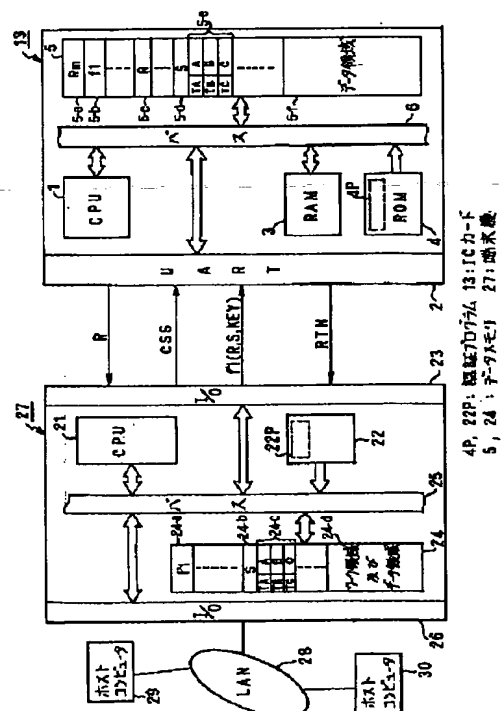
(74)代理人 弁理士 曾我 道照 (外6名)

(54)【発明の名称】 ICカードと端末機との間の認証方法およびそのシステム

(57)【要約】

【目的】 ICカードと端末機との間での認証を、認証コード或はこのアドレスを直接、双方の間で伝送することなく行うことにより、セキュリティの高い認証方法を得ることを目的とする。

【構成】 それぞれ対応する時間情報を有する複数の認証コード、および暗号化アルゴリズムをICカードおよび端末機の双方がそれぞれ格納しており、ICカードおよび端末機的一方で1つの認証コードを選択してこれを暗号化アルゴリズムで暗号化して認証データとして他方へ送ると共に、コマンド間或は信号間の時間を利用して選択された認証コードに対応する時間情報を他方へ送る。他方では、送られた時間情報から割り出された認証コードを同様に暗号化アルゴリズムにより暗号化して認証データを発生し、他方からの認証データと比較する。



【特許請求の範囲】

【請求項1】 ICカードおよび端末機がそれぞれ、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタイマ手段を有し、上記ICカードおよび端末機的一方がさらに乱数を発生する手段および比較手段を有する上記ICカードおよび端末機の間で認証を行う、ICカードと端末機との間の認証方法であって、ICカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、

上記他方の装置において、受信した乱数を上記複数の認証コードのうちの1つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第1暗号化工程と、

上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記暗号化された認証データを一方の装置に送信する工程と、

上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する第2暗号化工程と、上記一方の装置において、上記第2暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、

を備えたICカードと端末機との間の認証方法。

【請求項2】 上記ICカードおよび端末機のうちの上記他方の装置が上記乱数受信後にカウント開始信号を上記一方の装置に送信する工程をさらに含み、上記認証データ送信工程では、上記カウント開始信号送信後、使用した上記認証コードに対応する時間情報の時間が経過した後に上記認証データが一方の装置に送信され、上記第2暗号化工程では、上記一方の装置で上記カウント開始信号を受信した時から上記認証データを受信するまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に暗号化する請求項1のICカードと端末機との間の認証方法。

【請求項3】 上記認証データ送信工程では、上記ICカードおよび端末機のうちの上記他方の装置において上記乱数を受信後、使用した上記認証コードに対応する時間情報の時間が経過した後に上記認証データが一方の装置に送信され、上記第2暗号化工程では、上記一方の装置において上記乱数を送信した時から上記認証データを受けた時までの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に暗号

化する請求項1のICカードと端末機との間の認証方法。

【請求項4】 上記ICカードが上記アルゴリズムを予め格納していない場合に、上記認証作業の乱数送信工程の前に、上記暗号化用のアルゴリズムを上記端末機からICカードへロードするアルゴリズムロード工程をさらに含む請求項1のICカードと端末機との間の認証方法。

【請求項5】 上記第1暗号化工程において、ICカードと端末機とのランザクションの回数をカウントし、所定の値に達した時に選択する認証コードを変える請求項1のICカードと端末機との間の認証方法。

【請求項6】 上記ICカードおよび端末機がそれぞれN個の認証コードを有し、上記第1暗号化工程において、上記乱数をNで割り、余りをmとすると、m+1番目の認証コードを選択するようにした請求項1のICカードと端末機との間の認証方法。

【請求項7】 ICカードと端末機とがそれぞれ、対応する識別子をそれぞれ有する複数の認証コード、複数のアルゴリズム、これらのアルゴリズムに従ってデータの暗号化を行う暗号化手段をそれぞれ有し、上記ICカードと端末機的一方がさらに乱数を発生する手段、複合化手段および比較手段を有する上記ICカードおよび端末機の間で認証を行う、ICカードと端末機との間の認証方法であって、

ICカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、

上記他方の装置において、受信した乱数を上記複数の認証コードのうちの1つの認証コードをキーとして第1のアルゴリズムに従って暗号化して認証データを発生すると共に、第2のアルゴリズムに従って上記認証コードの識別子を暗号化する第1暗号化工程と、

この第1暗号化工程で作られた暗号化されたデータをそれぞれ上記一方の装置に送信する工程と、

上記一方の装置において上記識別子を暗号化したデータを複合化して対応する認証コードを得るための複合化工程と、

この複合化工程で得られた認証コードをキーとして、上記乱数を上記他方の装置と同様に第1のアルゴリズムに従って暗号化して認証データを発生する第2暗号化工程と、

この第2暗号化工程で生成された認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を他方の装置へ送信する工程と、

を備えたICカードと端末機との間の認証方法。

【請求項8】 双方の間の認証作業を行うICカードおよび端末機からなるシステムであって、

上記ICカードおよび端末機がそれぞれ、

少なくとも1つの暗号化用のアルゴリズム、少なくとも

1つのシステムキー、それぞれ対応する時間情報を有する複数の認証コード、および認証作業を行うための認証プログラムを含むプログラムを格納した記憶手段と、データの入出力制御を行う入出力制御手段と、上記記憶手段に格納されたプログラムに従ってデータの処理および制御を行うと共に、上記認証プログラムに従って認証作業を行うデータ制御・処理手段と、時間をカウントするタイマ手段と、上記各手段を接続するバス手段と、を備え、上記ICカードおよび端末機の一方向の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、乱数を発生して他方の装置に送信する手段と、所定の信号が送信された時から、上記他方の装置からの暗号化された認証データを受けた時までの間の時間間隔を上記タイマ手段によりカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する暗号化手段と、この暗号化手段で作られた認証データと上記他方の装置から送信された認証データとを比較して、上記他方の装置へ一致したか否かを示す結果信号を送信する手段と、を備え、上記ICカードおよび端末機の他方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、上記一方の装置から受けた乱数を上記複数の認証コードのうちの1つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する暗号化手段と、この暗号化手段で作られた認証データを、上記所定の信号が送信された時から、使用した上記認証コードに対応する時間情報の時間が経過後に上記一方の装置に送信する手段と、を備えたICカードおよび端末機からなるシステム。

【請求項9】 上記カウントの基準となる上記所定の信号が上記一方の装置から他方の装置に送信される上記乱数である請求項8のICカードおよび端末機からなるシステム。

【請求項10】 上記ICカードおよび端末機の上記他方の装置が、上記一方の装置に対してカウント開始信号を送信する手段を有し、上記カウントの基準となる上記所定の信号が上記カウント開始信号である請求項8のICカードおよび端末機からなるシステム。

【請求項11】 上記ICカードが上記アルゴリズムを予め格納していない場合に、上記端末機が、上記アルゴリズムを上記ICカードへロードするアルゴリズムロード手段をさらに含む請求項8のICカードおよび端末機からなるシステム。

【請求項12】 上記他方の装置が、ICカードと端末

機とのトランザクションの回数をカウントし、所定の値に達した時に選択する認証コードを変える認証コード選択手段をさらに備えた請求項8のICカードおよび端末機からなるシステム。

【請求項13】 上記ICカードおよび端末機がそれぞれN個の認証コードを有し、上記他方の装置が、上記乱数をNで割り、余りをmとすると、m+1番目の認証コードを選択する認証コード選択手段をさらに備えた請求項8のICカードおよび端末機からなるシステム。

10 【請求項14】 双方の間の認証作業を行うICカードおよび端末機からなるシステムであって、上記ICカードおよび端末機がそれぞれ、複数の暗号化用のアルゴリズム、複数のシステムキー、それぞれ対応する識別子を有する複数の認証コード、および認証作業を行うための認証プログラムを含むプログラムを格納した記憶手段と、データの入出力制御を行う入出力制御手段と、上記記憶手段に格納されたプログラムに従ってデータの処理および制御を行うと共に、上記認証プログラムに従って認証作業を行うデータ制御・処理手段と、

20 上記各手段を接続するバス手段と、を備え、上記ICカードおよび端末機の一方向の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、乱数を発生して他方の装置に送信する手段と、上記他方の装置から送信される上記識別子を暗号化したデータを複合化して対応する認証コードを得る識別子複合化手段と、

30 この識別子複合化手段で得られた認証コードをキーとして、上記乱数を上記他方の装置と同様に第1のアルゴリズムに従って暗号化して認証コードを発生する暗号化手段と、この暗号化手段で作られた認証データと、上記他方の装置から送信された第1のアルゴリズムにより暗号化された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する手段と、を備え、上記ICカードおよび端末機の他方の装置がさらに、上記認証プログラムに従って上記データ制御・処理手段の制御によりそれぞれ行われる、

40 上記一方の装置から受けた乱数を上記複数の認証コードのうちの1つの認証コードをキーとして第1のアルゴリズムに従って暗号化して認証データを発生すると共に、第2のアルゴリズムに従って上記認証コードの識別子を暗号化する暗号化手段と、

この暗号化手段で作られた暗号化されたデータをそれぞれ上記一方の装置に送信する手段と、を備えたICカードおよび端末機からなるシステム。

【請求項15】 2つの電氣的装置が、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタ

50

イマ手段をそれぞれ有し、両者の一方がさらに乱数を発生する手段および比較手段を有する、2つの電氣的装置間で認証を行う認証方法であって、

上記2つの装置の上記一方の装置で乱数を発生し他方へ送信する工程と、

上記他方の装置において、受信した乱数を上記複数の認証コードのうちの1つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第1暗号化工程と、

上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記認証データを一方の装置に送信する工程と、

上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証コードを発生する第2暗号化工程と、上記一方の装置において、上記第2暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、

を備えた2つの電氣的装置の間の認証方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、ICカードと端末機との間の認証方法およびそのシステムに関する。

【0002】

【従来の技術】ICカードと端末機との間の認証方法の従来技術として、例えば特開昭59-77575号公報(特公平3-40879号公報)に開示されているものがある。この従来技術で示されている認証方法は、まず端末機側で乱数を発生させ、この乱数とカードに記憶されている目的の認証コードを特定するためのアドレスをカード側に送る。ICカード側では与えられたアドレスより該当する認証コードを割り出す。そしてICカード自身が持っている暗号器を使用して、与えられた乱数と割り出された認証コードを使って所定の処理を行い処理結果を導き出し、この結果を端末機側に送信する。端末機も認証コードに関する情報および暗号器をICカードと同様に備えており、これを使用して乱数と認証コードからICカードと同様の処理を行う。そしてこの処理結果とICカードから送られて来た処理結果が一致すれば、該ICカードを正当なものであると判断している。

【0003】

【発明が解決しようとする課題】従来のICカードと端末機との間の認証は以上のように行われていたが、目的の認証コードを得るために、端末機からICカードへ認証コードが格納されている番地を示すアドレスを直接的に与えているために、不正使用者に認証コードが格納さ

れている場所および内容を知られてしまう危険性があるという問題点があった。

【0004】この発明は上記のような問題点を解消するためになされたもので、不正使用者にICカード内の認証コードが格納されている番地(アドレス)およびその内容が知られることのない認証方法およびそのシステムを得ることを目的とする。

【0005】

【課題を解決するための手段】上記の目的に鑑み、この発明は、ICカードおよび端末機がそれぞれ、対応する時間情報をそれぞれ有する複数の認証コード、所定のアルゴリズムに従ってデータを暗号化する暗号化手段、およびタイマ手段を有し、上記ICカードおよび端末機の一方がさらに乱数を発生する手段および比較手段を有する上記ICカードおよび端末機の間で認証を行う、ICカードと端末機との間の認証方法であって、ICカードおよび端末機の上記一方の装置で乱数を発生し他方へ送信する工程と、上記他方の装置において、受信した乱数を上記複数の認証コードのうちの1つの認証コードをキーとして上記アルゴリズムに従って暗号化して認証データを発生する第1暗号化工程と、上記他方の装置において、所定の信号が送信された後、使用した上記認証コードに対応する時間情報の時間が経過後に上記暗号化された認証データを一方の装置に送信する工程と、上記一方の装置において、上記所定の信号が送信された後、上記他方の装置から認証データを受けるまでの間の時間間隔をカウントし、カウントされた時間間隔と一致する時間情報に対応する認証コードをキーとして、上記乱数を上記他方の装置と同様に上記アルゴリズムに従って暗号化して認証データを発生する第2暗号化工程と、上記一方の装置において、上記第2暗号化工程で作られた認証データと、上記他方の装置から送信された認証データとを比較して、一致したか否かを示す結果信号を上記他方の装置へ送信する工程と、を備えたICカードと端末機との間の認証方法にある。

【0006】また、この発明の別の実施例では、複数の認証コードに時間情報の代わりに識別子をそれぞれ割り当て、この識別子を暗号化して送り、受けた側ではこれを複合化して求められた識別子から選択された認証コードを割り出し、この認証コードをキーとして乱数を暗号化して認証データを発生し、送られてきた認証データと比較して認証を行う。また、この発明は上記認証方法を行うICカードおよび端末機からなる装置としてのシステムも含む。

【0007】

【作用】この発明に係る認証方法では、時間情報がそれぞれに割り当てられた複数の認証コードをICカードと端末機とがそれぞれ設け、一方で選択された認証コードを相手側に伝える際には、該認証データの対応する時間情報をコマンドとコマンドの間の時間間隔として相手側

に伝達し、受けた側ではコマンド間の時間間隔から対応する認証コードを割り出す。そしてICカードと端末機の双方で該認証コードをキーとして乱数を暗号化アルゴリズムに従って暗号化して認証データを発生し、これを比較して一致したことにより互いの正当性を確認する。

【0008】また別の実施例では複数の認証コードにそれぞれ識別子を割り当て、一方で選択された認証コードを相手側に伝える際には、該認証データの対応する識別子を識別子暗号化用のアルゴリズムで暗号化して相手側に伝達し、受けた側ではこれを複合化して識別子を求めて認証コードを割り出す。そしてICカードと端末機の双方で該認証コードをキーとして乱数を暗号化アルゴリズムに従って暗号化して認証データを発生し、これを比較して一致したことにより互いの正当性を確認する。

【0009】これらの認証方法では認証コードおよびこれのアドレスを直接的に双方の間で送ることがなく、不正使用者に認証コードを知られることなく認証作業を行うことができる。

【0010】

【実施例】以下、この発明の実施例を添付図面に基づいて説明する。図1はこの発明で使用されるICカードの機能的構成の一例を示す。図において、ICカード13はCPU1、入出力制御回路(以下UART)2、RAM3、ROM4、データメモリ5、内部バス6を備えている。UART2はI/O端子7でのデータの入出力制御をする。RAM3はCPU1で計算等に使用されるデータの一時記憶のためのメモリである。ROM4はCPU1を駆動させるためのプログラムが格納される読み出し専用のメモリである。データメモリ5はこの発明では、認証コード(IDコード)、認証コードテーブル、暗号化アルゴリズム、および一般的なデータ等を格納するためのメモリである。このデータメモリ5は通常、EEPROMからなる。内部バス6は上述した各機能ブロックを接続する。ICカード13はさらに電源端子8(Vcc)、クロック端子9(CLK)、リセット端子10(RST)およびグランド端子12(GND)を備えている。またタイマ回路12はタイムカウントを専門に行う回路で、本願のICカードはこれを内蔵する場合としない場合がある。

【0011】このICカード13のハードウェアの構造は従来のものと何等変わりなく、データメモリ5が他の部分と一体になったワンチップ構造のものと、他の部分と分離されたマルチチップ構造のものとがある。動作は、カード外部からI/O端子7、UART2、バス6を介して命令が与えられると、この命令に基づいてCPU1がROM4に格納されたプログラムに従って処理を行う。そしてその処理結果は、命令とは逆経路でカード外部へ出力される。この発明の認証作業(照合作業)についても同様に行われる。

【0012】図2はこの発明の第1実施例で使用されるICカードと端末機からなるシステムの機能的構成を示

すブロック図である。図2においてICカード13は図1に示したものである。ICカード13のデータメモリ5の内部には様々なデータが格納されている。領域5-aには乱数発生アルゴリズム(Rm)、領域5-bには暗号化アルゴリズム(f1)、領域5-cには乱数発生アルゴリズム(Rm)によって発生する乱数(R)、領域5-dには暗号化アルゴリズム(f1)に使用されるシステムキー(S)、領域5-eには認証を行うための複数の認証コード(A、B、C...)とこれらのそれぞれに割り当てられ時間情報(TA、TB、TC...)の関係を示すテーブルがそれぞれ格納されている。また領域5-fは一般のアプリケーション等を使用されるデータ領域である。認証コード(A、B、C...)が格納された領域5-eの構成は図3に拡大して示した。テーブルはTIME72およびKEY73から構成されており、KEY73の個々の認証コード(A、B、C...)には、TIME72の時間情報(TA、TB、TC...)がそれぞれ割り付けられている。そして認証コードをKEYとして、対応する時間情報が割り出される。

【0013】また図2において、端末機27はICカード13との認証を行う端末機で、1つの端末機単独の場合もあれば、図示のように上位ホストコンピュータ29、30が接続されているLAN28に接続されている場合もある。端末機27の構成はICカード13とほぼ同様なものとなっており、バス25を介してCPU21、ROM22、データおよびワーク領域のためのデータメモリ24、入出力を制御するためのI/O(入出力制御回路)23、26が図示のように接続されている。データメモリ24はICカード13のデータメモリ5と同様に様々なデータを格納している。領域24-aには暗号化アルゴリズム(f'1)、領域24-bには暗号化アルゴリズム(f'1)に使用されるシステムキー(S)、領域24-cには認証を行うための認証コード(A、B、C...)がそれぞれ格納されている。また領域24-dは、一般のアプリケーション等やCPU21の一時記憶に使用されるワーク領域およびデータ領域である。認証コード(A、B、C...)が格納された領域24-cは図3に示したICカード13のデータメモリ5内の認証コードが格納された領域5-eと全く同じである。

【0014】図4および図5には図2のシステムのICカードと端末機との間で行われるこの発明の第1実施例による認証作業(動作)を説明するためのフローチャートを示した。図4はICカード27の動作のフローチャート、図5は端末機27の動作のフローチャートである。これらの動作は、端末機27およびICカード13のCPU21、4により、それぞれのROM22、4に格納された認証作業用の認証プログラム22P、4Pに従って行われる。

【0015】以下に図2～図5に従ってこの発明の第1実施例の動作を説明する。この第1実施例における認証

方法を概略的に説明すると、まず、ＩＣカード１３側で乱数(R)を発生させてこれを端末機２７側へ送る。端末機２７側では認証の目的の認証コード(KEY)と暗号化のためのシステムキー(S)を利用して暗号化アルゴリズム、例えば暗号化アルゴリズム(f' 1)の関数に基づいて暗号化された認証データ f' 1(R, S, KEY)を作り出し、ＩＣカード１３側へ認証のためのデータとして送り返す。なお、ここでの認証コード(KEY)は必ずしも実際の認証コードそのものである必要はなく、図面ではA、B、C...として示した。ＩＣカード１３側は、ＩＣカード１３自身がデータメモリ５の領域５-eに格納している認証コード(KEY)および、領域５-dに格納しているシステムキー(S)から端末機２７の暗号化アルゴリズム(f' 1)と同様の暗号化アルゴリズム(f 1)の関数に基づいて暗号化されたデータ f 1(R, S, KEY)を同様に作り出し、送られてきた暗号化されたデータすなわち認証データ f' 1(R, S, KEY)と照合する。

【００１６】この第１実施例では、目的の認証コードを相手側に知らせる方法に工夫を凝らし、例えばアドレス等で直接的に知らせるのではなく、コマンドとコマンドの間の時間間隔を利用することにより、相手側に認証コードを知らせようというものである。

【００１７】図４および図５のフローチャートに従ってもう少し詳しく説明する。図４のフローチャートに示すように、ＩＣカード１３はデータメモリ５の領域５-aに格納された乱数発生アルゴリズム(Rm)に従って乱数(R)を発生させ(ステップ４２)、端末機２７へ送信する(ステップ４３)。端末機２７は図５のフローチャートに示すように、乱数(R)を受信後(ステップ６２)、１つの認証コード(KEY)を選択して認証データ f' 1(R, S, KEY)を作り出す(ステップ６３)。そしてさらにデータメモリ２４の領域２４-cに格納されたタイムテーブル(図３参照)から選択した認証コード(KEY)(A、B、C...のいずれか)７３の対応する時間情報(TA、TB、TC...のいずれか)７２を割り出す。例えば、認証コードBを選択した場合には、その時間情報はTBというぐわいに割り出す(ステップ６４)。

【００１８】そして端末機２７とＩＣカード１３の時間の同期を図るために、端末機２７はＩＣカード１３へカウント開始信号CSSを送信し(ステップ６５)、端末機２７側のカウンタをリセットする(カウントを０にする)(ステップ６６)。端末機２７およびＩＣカード１３は同期のためのカウンタとして、専用のハードウェアとしてのタイマ回路１２(図１参照)をそれぞれ備えていてもいいし、あるいはCPUのソフトウェア上で行うカウンタ(特に図示せず)を使用してもよい。この第１実施例では、CPUのソフトウェア上で行うカウンタを使用したものとする。

【００１９】ＩＣカード１３もカウント開始信号(CSS)を受信後(ステップ４４)、ＩＣカード１３側のカウ

ンタをリセットし(カウントを０にする)(ステップ４５)、これにより端末機２７とＩＣカード１３との時間的同期を図る。端末機２７はカウント開始信号(CSS)を送信した後、タイムテーブルで設定されている時間情報の時間まで待ち(ステップ６７、６８、６９)、ＩＣカード１３へ認証データ f' 1(R, S, KEY)を送信する(ステップ７０)。ＩＣカード１３はカウント開始信号(CSS)受信から認証データ f' 1(R, S, KEY)を受信するまでの時間をカウントし(ステップ４６、４７、４８)、そのカウントした値からデータメモリ５の領域５-eに格納されたタイムテーブルに基づいて選択された認証コード、すなわち認証するための認証コードを割り出す(ステップ４９、５０、５１、５２、５３、５４)。

【００２０】そして該当する認証コード(KEY)より暗号化された認証データ f 1(R, S, KEY)を算出し(ステップ５５)、端末機２７より送信された認証データ f' 1(R, S, KEY)との照合を行う(ステップ５６、５７、５８)。そして照合の結果、双方の認証データが一致したか否かを示す結果信号(RTN)を端末機２７へ送信する(ステップ５９)。このようにすれば、直接的に認証コードが格納されているアドレスを端末機２７とＩＣカード１３間で送信することなく認証作業が行え、認証コードが格納されたアドレスを知られることなく、より安全に認証作業が行える。

【００２１】上記第１実施例では時間のカウントをCPUのソフトウェア上で行っていたが、ＩＣカードおよび端末機がそれぞれ専用のタイマ回路(図１の符号１２参照)を備えていてもよい。この場合、タイマ回路１２は例えば図６に示すようなフリップフロップを直列に接続したタイマカウンタのようなものでよい。

【００２２】図７はこの発明の第２実施例で使用されるＩＣカードと端末機からなるシステムの機能的構成を示すブロック図である。図２に示す第１実施例のものと異なる点は、ＩＣカード１３にハードウェアとしてのタイマ回路１２が設けられ、端末機２７にも同様のハードウェアとしてのタイマ回路３６が設けられている点、および端末機２７からＩＣカード１３へ送信されるカウント開始信号(CSS)が無い点である。また図８および図９には図７のシステムのＩＣカードと端末機との間で行われるこの発明の第２実施例による認証作業(動作)を説明するためのフローチャートを示した。

【００２３】次に図７～図９に従って第２実施例の動作を説明する。上記第１実施例ではソフトウェア上でカウント処理を行っているため、この第２実施例とは目的の認証コード(KEY)を断定するための時間情報を得る方法が異なる。この実施例では乱数の送信時にＩＣカード１３と端末機２７の同期をとるようにしている。図８および図９に示すように、ＩＣカード１３より乱数の送信が行われた後(ステップ８３)にＩＣカード１３および端

10

20

30

40

50

末機27でそれぞれタイマ回路12、36でカウントを開始する。ここで乱数がICカード13から送信されるのと、端末機27で乱数が受信されるのは同時とみなす。これは他の信号或はデータの送受信でも同様であり、また上記第1実施例でも同様である。そして上記乱数が送信された時点から、端末機27で作られた暗号化された認証データ $f'1(R, S, KEY)$ がICカード13で受信されるまでの時間をカウントし、この時間から目的の認証コード(KEY)を割り出すようにしている(ステップ87、88、89、90、91、92)。その他の処理は第1実施例と同様であり、説明は省略する。

【0024】上記第1および第2実施例では各認証コード(KEY)に対応する時間情報(TIME)を割り付け、この時間情報をコマンド間或は信号間の時間間隔として送るようにしていたが、複数の暗号化用アルゴリズムを利用して行う方法を以下に説明する。

【0025】図10はこの発明の第3実施例で使用されるICカードと端末機からなるシステムの機能的構成を示すブロック図である。図11には図10のICカード13のデータメモリ5内の領域5-eおよび端末機27のデータメモリ24の領域24-cの内容を示した。そして図12および図13には図10のシステムのICカードと端末機との間で行われるこの発明の第3実施例による認証作業(動作)を説明するためのフローチャートを示した。

【0026】図10のICカードと端末機からなるシステムにおいて、上記第1および第2実施例と異なる点は第1に、ICカード13のデータメモリ5に2つの暗号化用アルゴリズム $f1, g1$ および2つのシステムキー $S1, S2$ が格納されており、同様に端末機27のデータメモリ24にも2つの暗号化用アルゴリズム $f'1, g'1$ および2つのシステムキー $S1, S2$ が格納されている点である。第2にはデータメモリ5、24の領域5-e、24-cに、図11に示すテーブルが格納されている点である。このテーブルは各認証コード(KEY)にそれぞれ割り当てられた識別子(KID)を示すものである。

【0027】次に図10～図13に従って第3実施例の動作を説明する。ICカード13より乱数(R)が送信され(ステップ122)、端末機27でこの乱数(R)を受信すると(ステップ132)、端末機27では認証の目的の認証コード(KEY)を使用して上記実施例と同様に暗号化された認証データ $f'1(R, S1, KEY)$ を生成し(ステップ133)、同時に図11のテーブルから得られ該認証コード(KEY)の識別子(KID)を暗号化してデータ $g'1(KID, S2)$ を生成する(ステップ134)。そして生成された2つの認証データ $f'1(R, S1, KEY)$ および $g'1(KID, S2)$ をICカード13へ送信する(ステップ135)。

【0028】ICカード13はこれらの認証データを受

信後(ステップ123)、 $g'1(KID, S2)$ を複合化してKIDを求め(ステップ124)、このKIDからデータメモリ5に格納されたテーブルにより目的の認証コード(KEY)を得る(ステップ125)。そしてこの認証コードを使用して暗号化された認証データ $f1(R, S1, KEY)$ を算出し(ステップ126)、端末機27より送信された認証データ $f'1(R, S1, KEY)$ と照合を行い(ステップ127、128、129)、一致したか否かを示す結果信号(RTN)を端末機27へ送信する(ステップ130)。このようにすれば、外部に直接的な認証コードが格納されているアドレス等を知られることなく認証作業を行うことができる。

【0029】一般的にICカードはROM容量、RAM容量、データメモリ等のリソースに制限があり、暗号化アルゴリズム($f'1, g'1$)等のプログラムがICカード側に収めることができない場合もある。また、アプリケーションによっては複数の暗号化アルゴリズムを条件によって使い分けする場合もある。このような場合を想定してこの発明の第4実施例では、この問題を解決できるように、例えば認証作業の前に暗号化アルゴリズムを端末機27からICカード13へロードするようにした。

【0030】図14はこの発明の第4実施例で使用されるICカードと端末機からなるシステムの機能的構成を示すブロック図である。図10に示された第3実施例のものと異なる点は、ICカード13のデータメモリ5内に暗号化アルゴリズム $f1, g1$ が格納されていない点である。また図15は図14のシステムのICカードと端末機との間で行われるこの発明の第4実施例による認証作業(動作)におけるICカードの動作のフローチャートを示した。

【0031】この実施例では、ICカード13から乱数(R)を発生した後(ステップ142)、端末機27側からICカード13へ暗号化アルゴリズム($f'1, g'1$)を送信し(ステップ143)する。ICカード13ではRAM3の領域3-aおよび3-b、もしくはデータメモリ5の空き領域5-iおよび5-jにこれらの暗号化アルゴリズム($f'1, g'1$)をロードする(ステップ144)。そしてその後、上記実施例で行われている認証処理(作業)を行うようにした(ステップ145)。なお、認証処理の前に暗号化アルゴリズムを端末機側からICカード側へ送信することは、上記各実施例に適用可能である。

【0032】また、ICカードと端末機間のトランザクション上のセキュリティを高めるために、トランザクションの回数をカウントし、ある設定値、例えば100回に達した時に、別の認証コードによる認証を必要とするようにした実施例を以下に示す。

【0033】図16～18はこの発明の第5実施例によるICカードと端末機との間の認証方法を示すフローチ

10

20

30

40

50

ャートであり、図17および図18は図16中のそれぞれ送信処理、受信処理を詳しく示している。以下図に従って第5実施例の動作を説明する。

【0034】この実施例では、ICカードと端末機との間のトランザクションの回数は、例えば第1実施例を示す図2のICカード13のCPU1もしくは端末機27のCPU21でトランザクションの回数をインクリメントするなどしてカウントする。そして最初の認証処理(図16のステップ153)が行われる前に、CPUのトランザクションカウンタをリセットする(ステップ152)。その後、様々の処理が行なわれる中でICカード13と端末機27との間にデータの送受信が発生する。その送信および受信の回数をカウントしながら認証を行う。

【0035】図17は図16中の送信処理(ステップ154)での詳細の動作を示す。送信する前にはトランザクションカウンタを+1だけインクリメントし(ステップ162)、トランザクションの回数が100回に達したか否かを判断する(ステップ163)。100回に達していれば別の認証コードによる認証処理を行い(ステップ164)、認証処理で認証が正しく行われればデータを送信し、その後、トランザクションカウンタをリセットする(ステップ167、168、169)。また100回に達していなければそのままデータを送信する(ステップ165)。

【0036】一方、受信処理(ステップ155)の場合は、図18に示すようにデータの受信後(ステップ172)、トランザクションカウンタを+1だけインクリメントし(ステップ173)、トランザクションの回数が100回に達したか否かを判定する(ステップ174)。100回に達していれば別の認証コードで認証処理を行い(ステップ175)、その後、トランザクションカウンタをリセットする(ステップ176)。また100回に達していなければそのまま次の処理に移行する。

【0037】また、複数の認証コード(KEY)を持つ場合に、認証に使用する認証コードをランダムに選択する方法を付加することにより、より一層セキュリティの高いものが実現できる。図19には乱数を利用して認証コードをランダムに選択する機能を付加した、この発明の第6実施例による認証方法の動作を示すフローチャートが示されている。以下、この動作について説明する。

【0038】例えば認証コード(KEY)(A、B、C...)の数がN個である場合には、乱数(R)を認証コード(KEY)の個数N個で割り、残りmを求め(ステップ183)、m+1番目の認証コード(KEY)を選択することにより(ステップ184~189)、ランダムに認証コードを選択することができる。例えば、m=0なら1番目の認証コード(A)、m=1なら2番目の認証コード(B)という様に選択する。

【0039】なお上記各実施例の説明において、ICカ

ード側および端末機側のいずれかを限定して説明した事項は、ICカード側および端末機側の限定を逆にしても同様の認証を行うことができる。例えば乱数発生はICカード側で行っているが、端末機側で行ってもよい。また、上記実施例ではICカードと端末機との間の認証方法について説明したが、この発明は認証を必要とする2つの装置間であれば、どのような形態でも適用可能である(例えば、端末機と端末機間、システムとシステム間)。

【0040】

10 【発明の効果】以上説明したように、この発明によれば、ICカードと端末機との間で、認証コード或は認証コードが記憶されているアドレスを直接伝送することなく認証作業を行うようにしたので、不正使用者に認証コードの内容やアドレスを知られることがなく、セキュリティの非常に高い認証方法およびそのシステムが得られる効果がある。

【図面の簡単な説明】

【図1】この発明で使用されるICカードの機能的構成を一例を示すブロック図である。

20 【図2】この発明の第1実施例によるICカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図3】図2のICカードおよび端末機のデータメモリ内に格納された認証コードと対応する時間情報の内容を拡大して示した図である。

【図4】この発明の第1実施例による認証方法におけるICカードの動作を示すフローチャート図である。

【図5】この発明の第1実施例による認証方法における端末機の動作を示すフローチャート図である。

30 【図6】タイマ回路の一例を示す図である。

【図7】この発明の第2実施例によるICカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図8】この発明の第2実施例による認証方法におけるICカードの動作を示すフローチャート図である。

【図9】この発明の第2実施例による認証方法における端末機の動作を示すフローチャート図である。

40 【図10】この発明の第3実施例によるICカードと端末機からなるシステムの機能的構成を示すブロック図である。

【図11】図10のICカードおよび端末機のデータメモリに格納された認証コードと対応する時間情報の内容を拡大して示した図である。

【図12】この発明の第3実施例による認証方法におけるICカードの動作を示すフローチャート図である。

【図13】この発明の第3実施例による認証方法における端末機の動作を示すフローチャート図である。

50 【図14】この発明の第4実施例によるICカードと端末機からなるシステムの機能的構成を示すブロック図である。

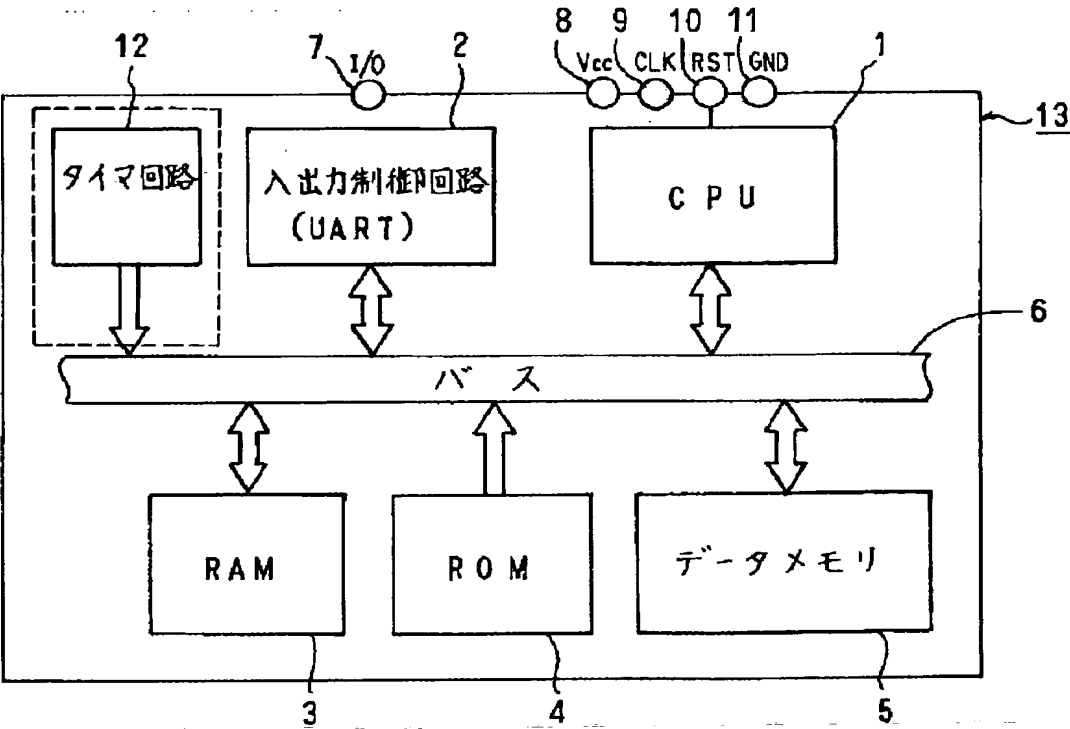
【図15】この発明の第4実施例による認証方法におけるICカードの動作を示すフローチャート図である。
【図16】この発明の第4実施例によるICカードと端末機との間の認証方法を示すフローチャートである。
【図17】図16中の送信処理の詳細な動作を示すフローチャートである。
【図18】図16中の受信処理の詳細な動作を示すフローチャートである。
【図19】この発明の第6実施例による認証方法における動作を示すフローチャート図である。

【符号の説明】

1 CPU

- 2 UART(入出力制御回路)
- 3 RAM
- 4 ROM
- 5 データメモリ
- 6 バス
- 13 ICカード
- 21 CPU
- 22 ROM
- 23 I/O
- 24 データメモリ
- 26 I/O
- 27 端末機

【図1】



13 : ICカード

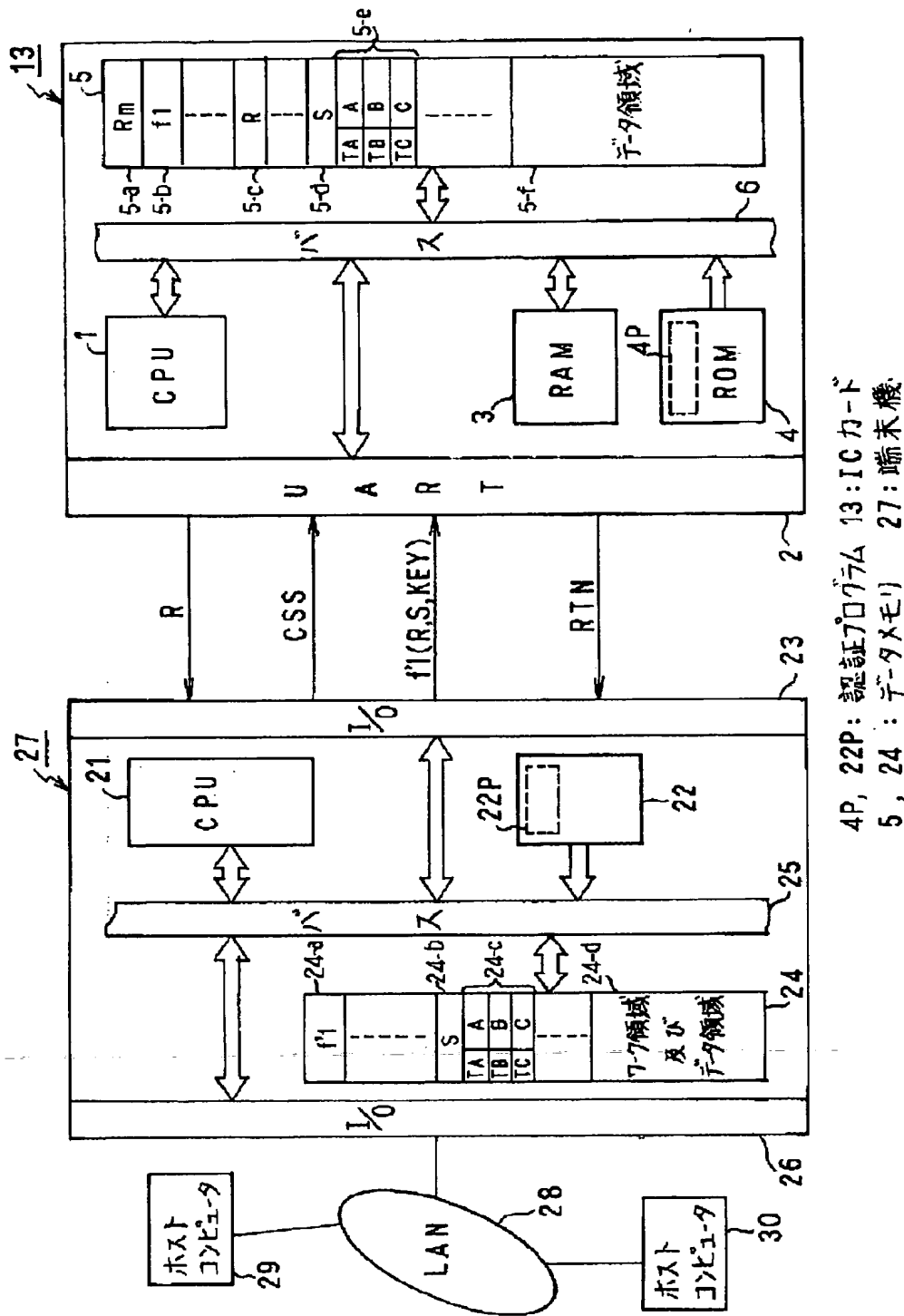
【図3】

TIME (72)	KEY (73)	5-e, 24-c
TA	A	
TB	B	5-e, 24-c
TC	C	
TD	D	5-e, 24-c

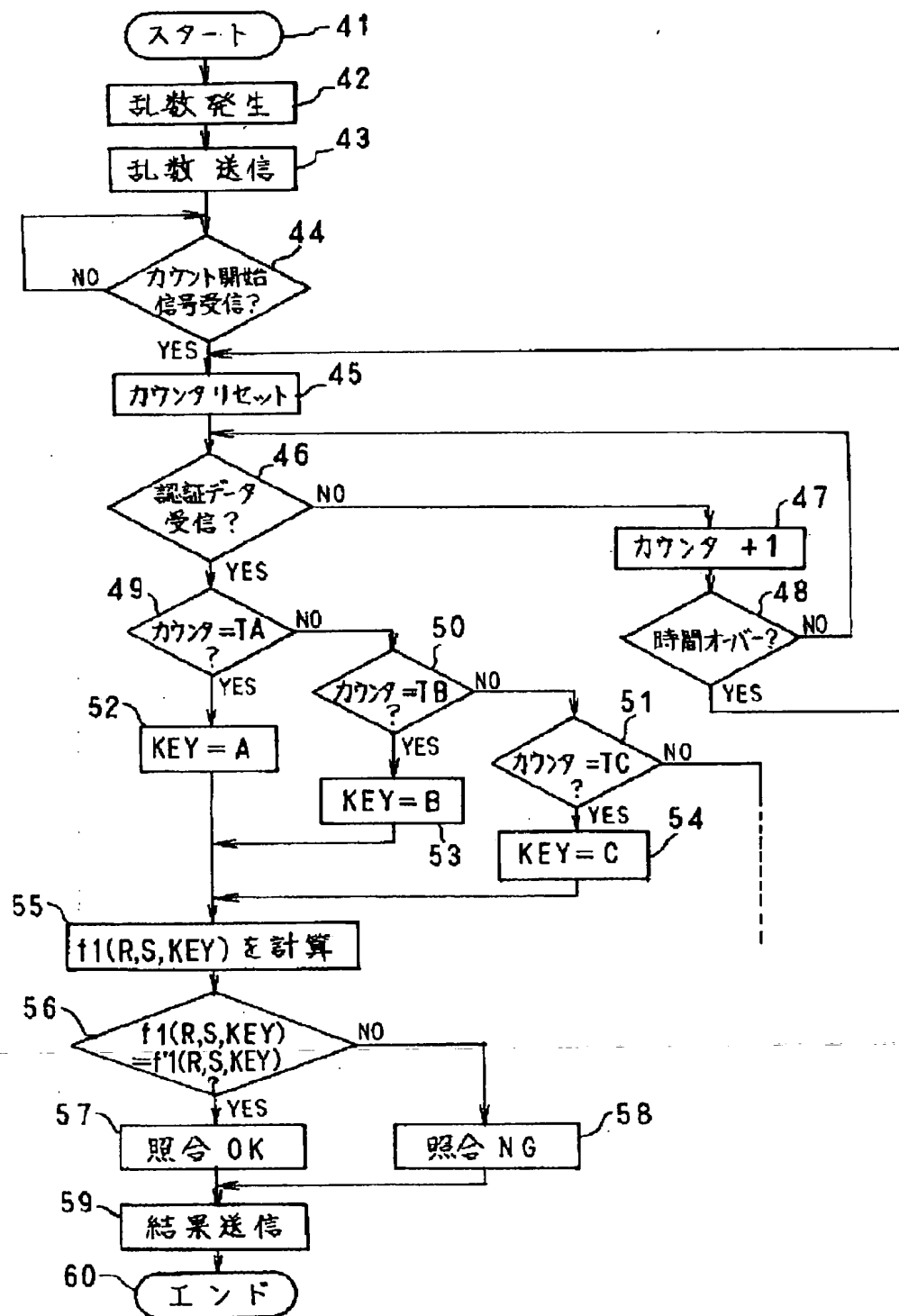
【図11】

KID (74)	KEY (73)	5-e, 24-c
KA	A	
KB	B	5-e, 24-c
KC	C	
KD	D	5-e, 24-c

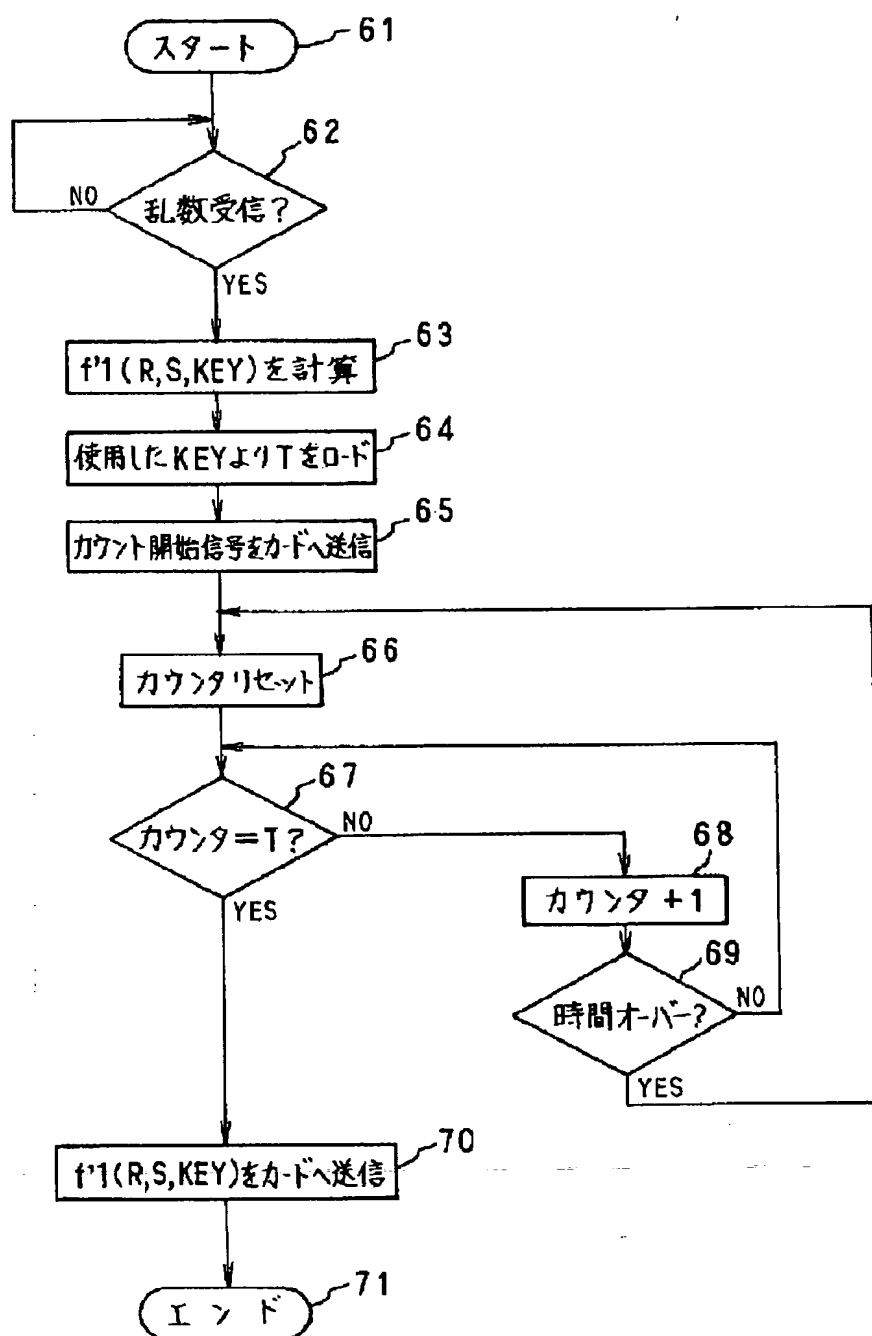
【図2】



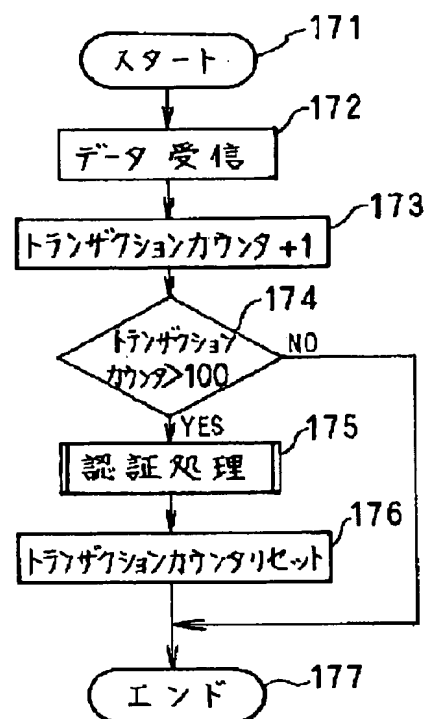
【図4】

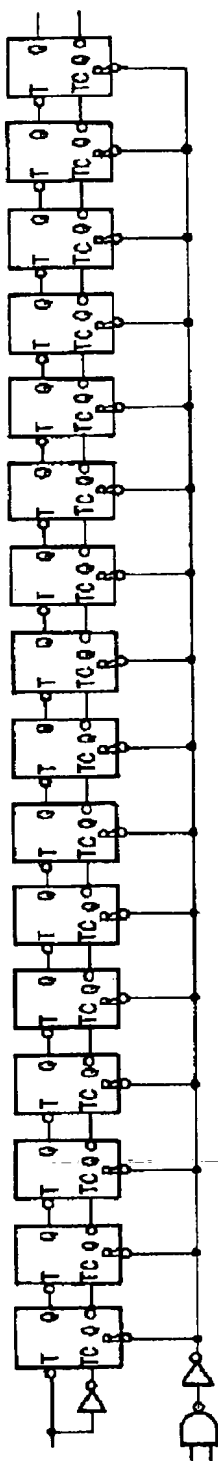


【図5】

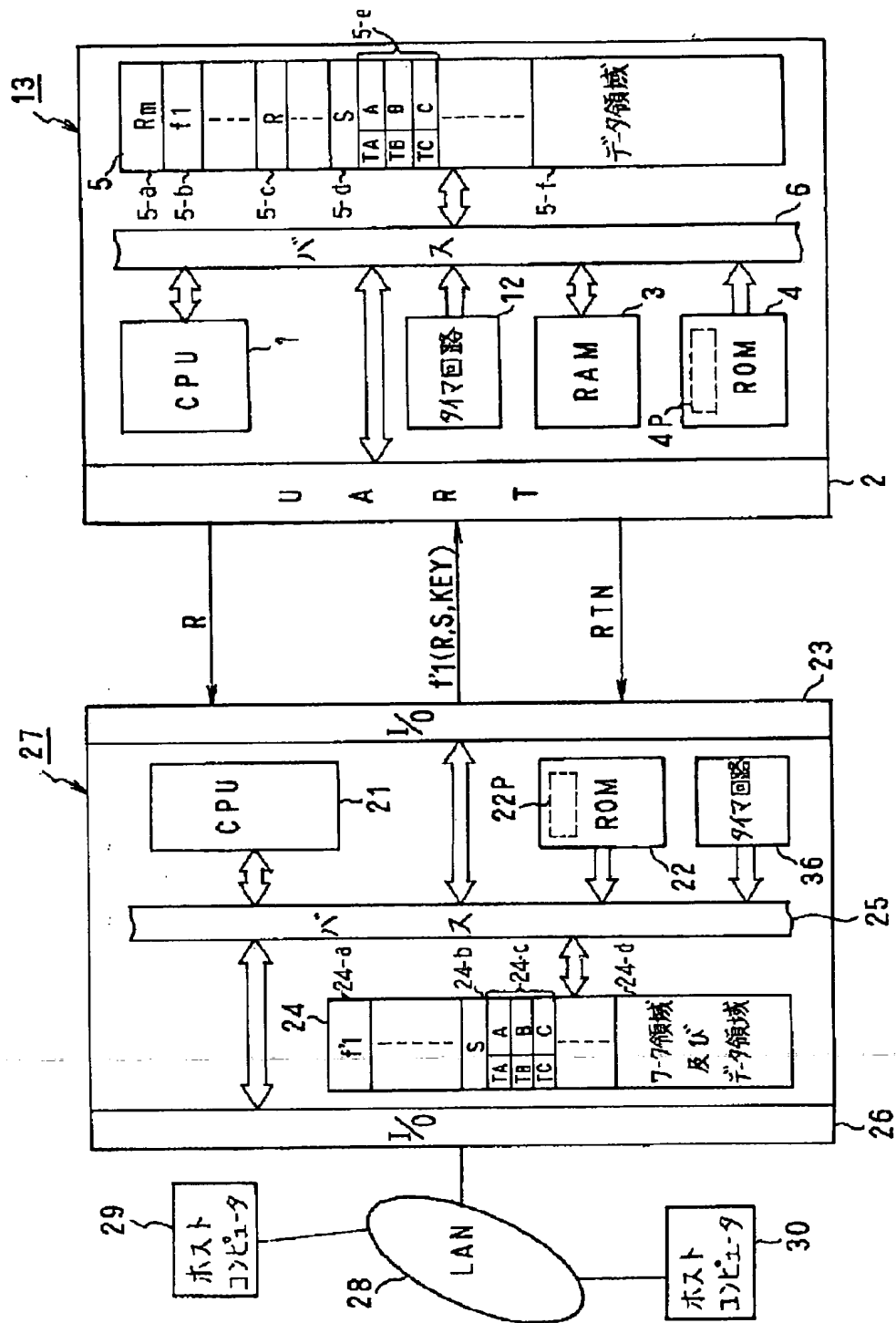


【図18】

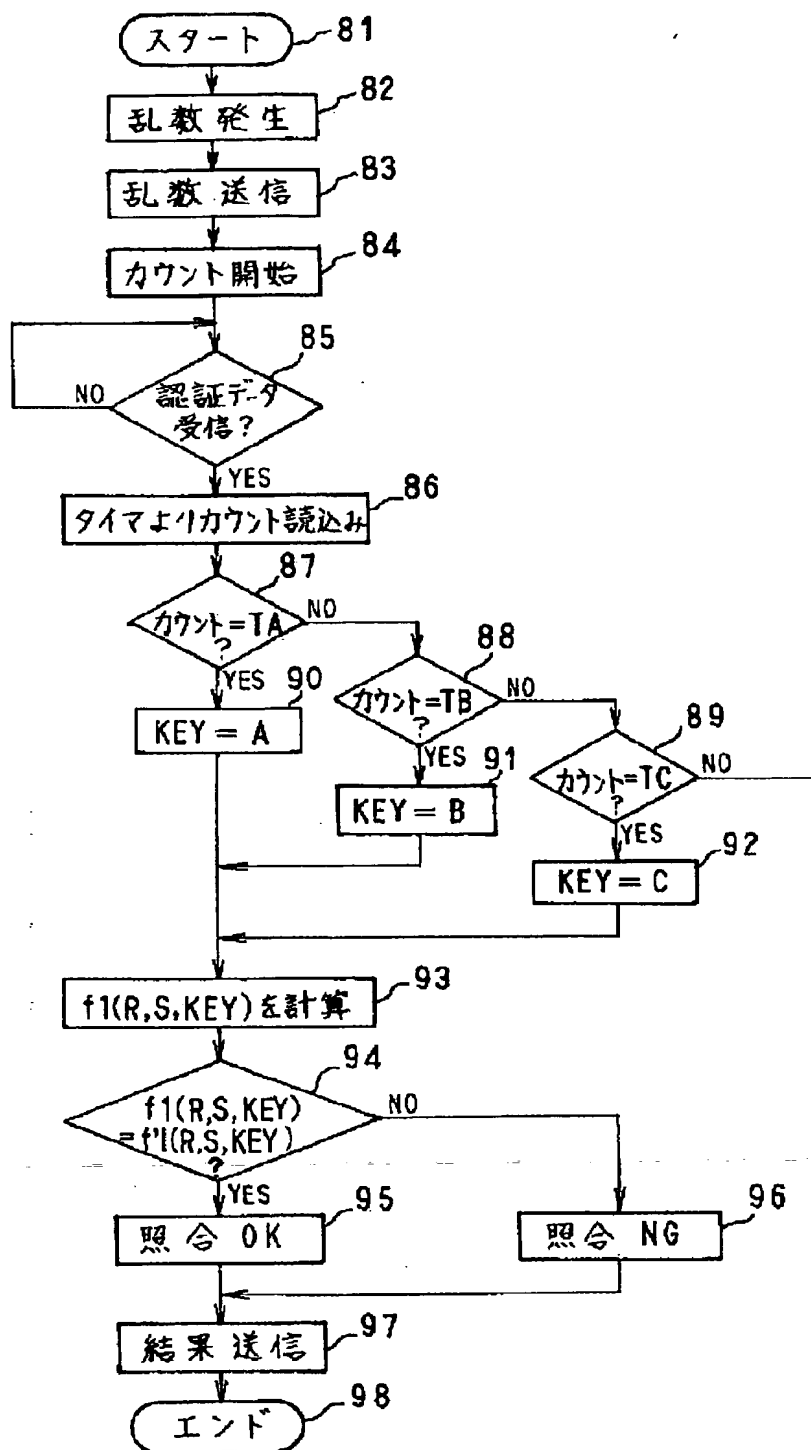




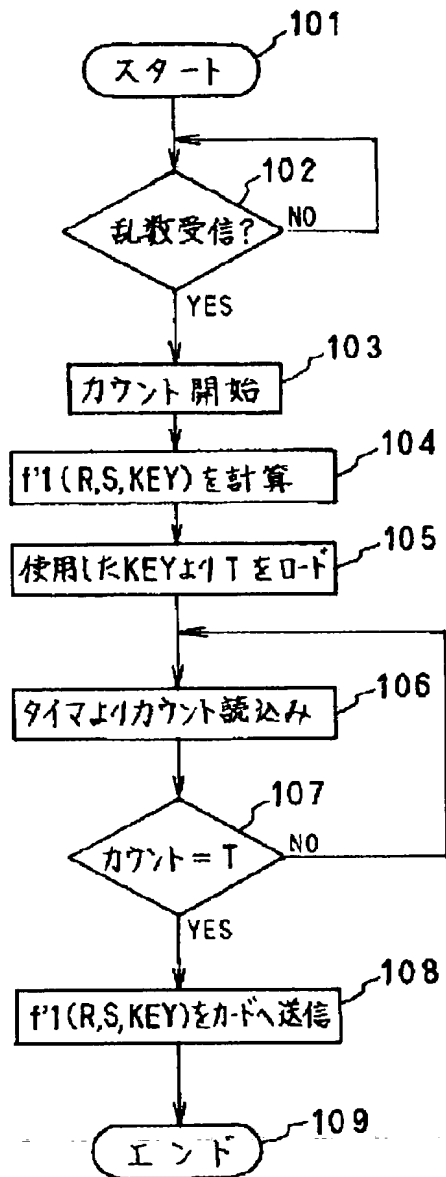
【図7】



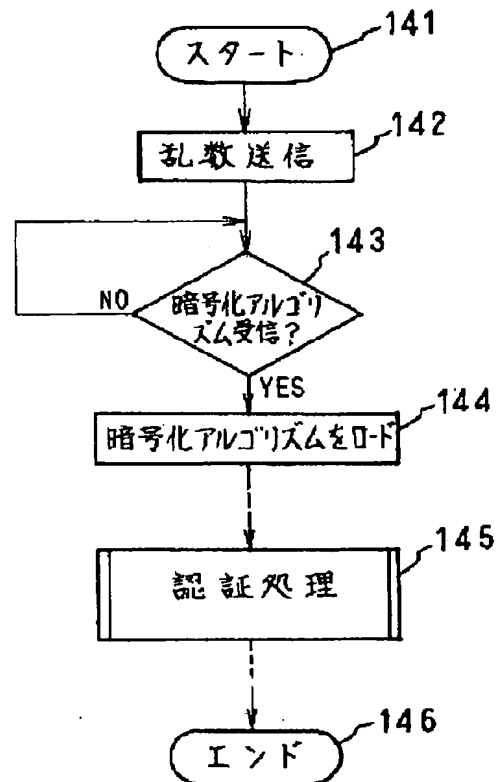
【図8】



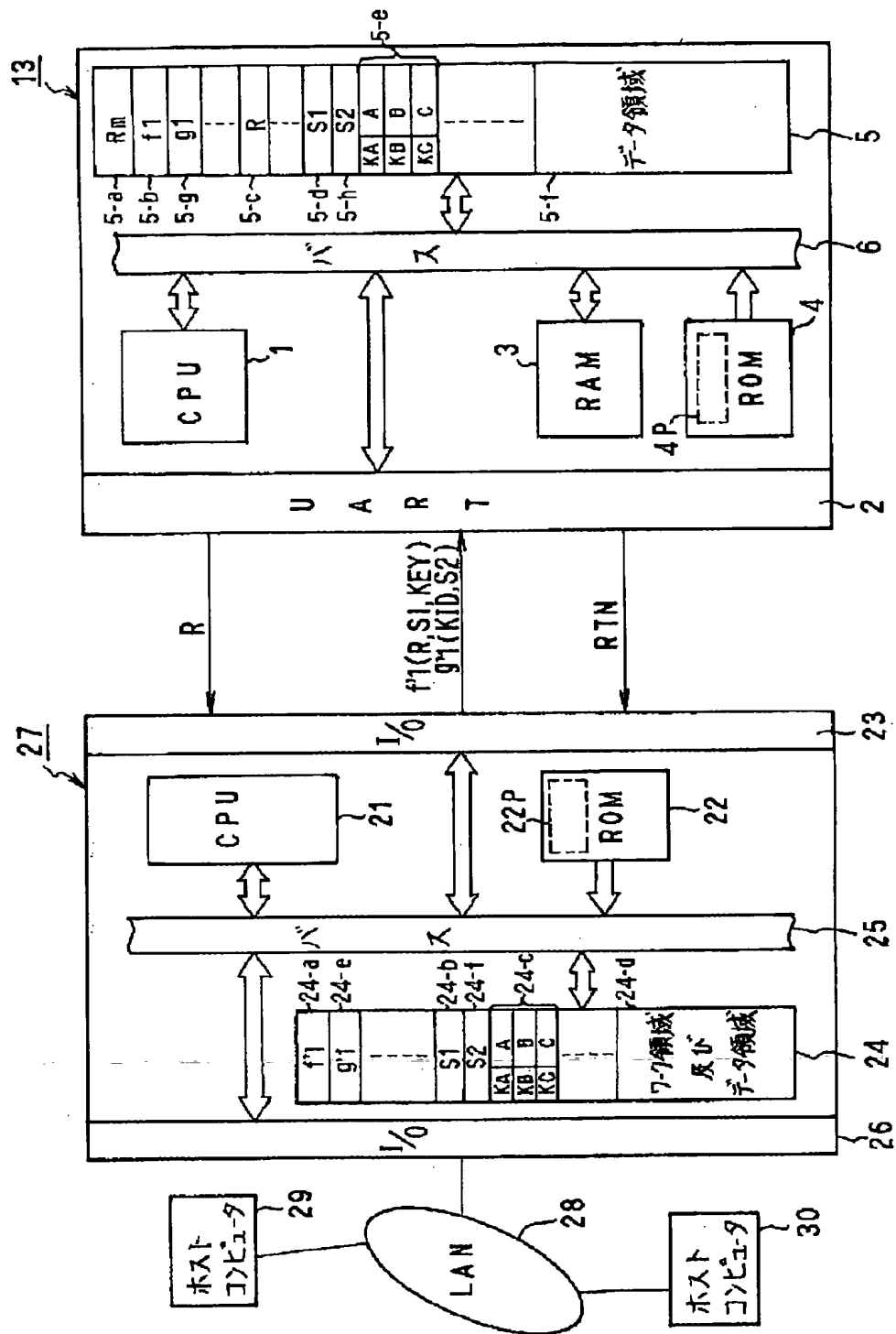
【図9】



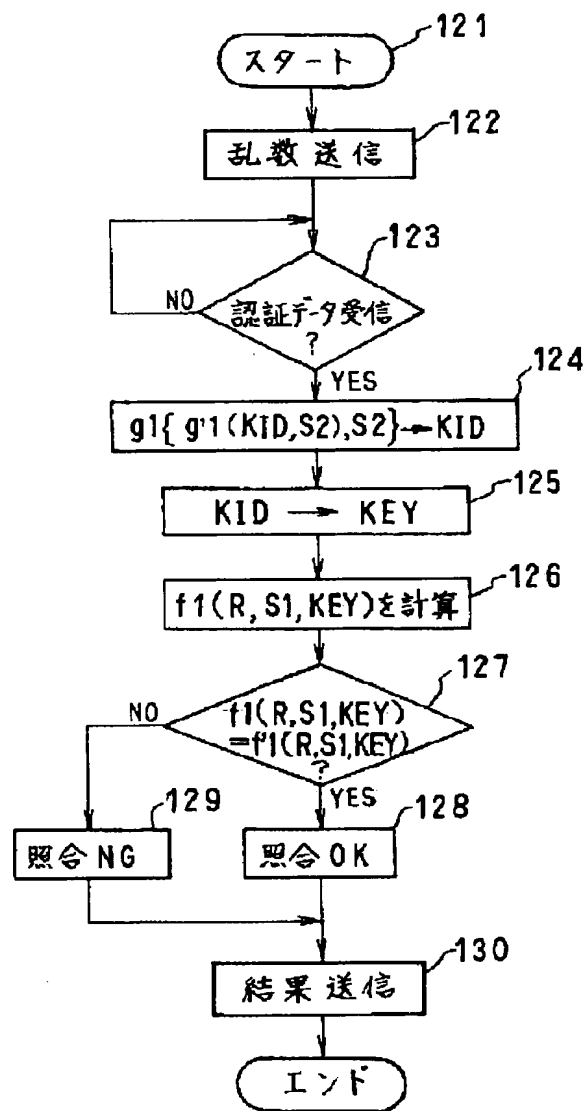
【図15】



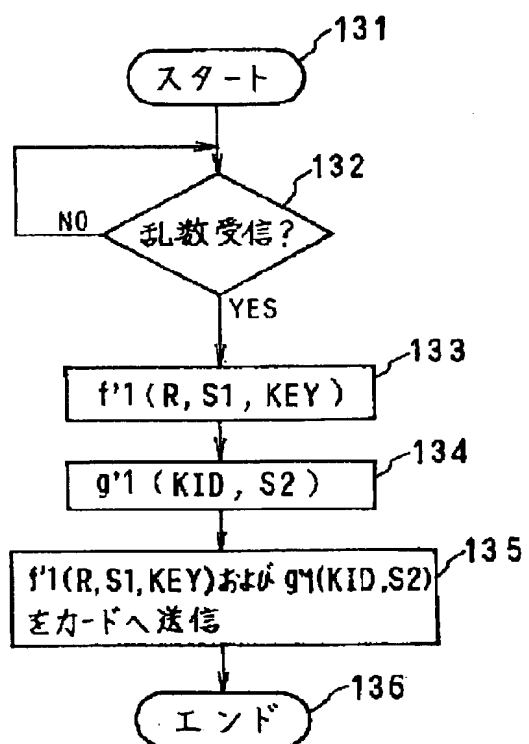
【図10】



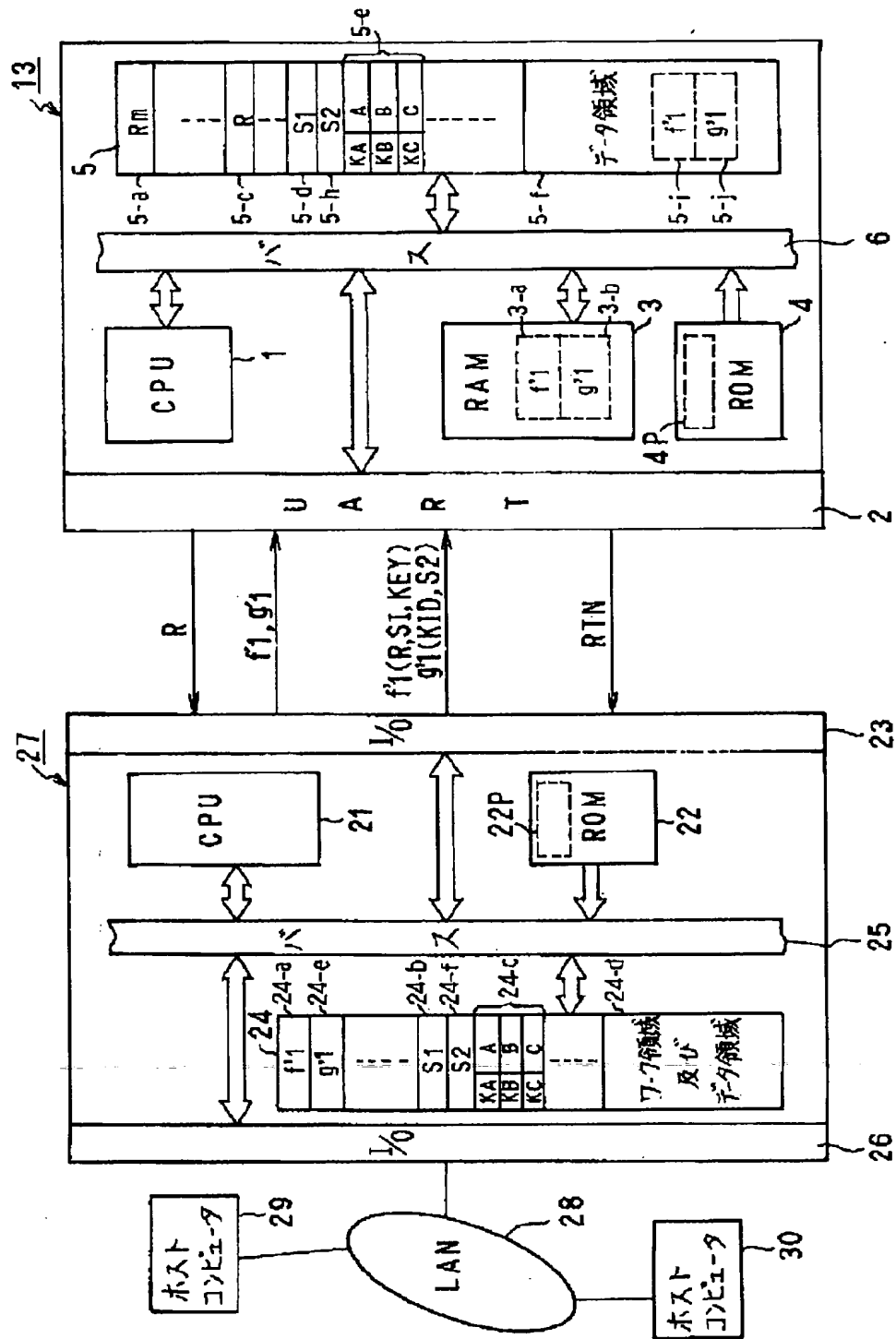
【図12】



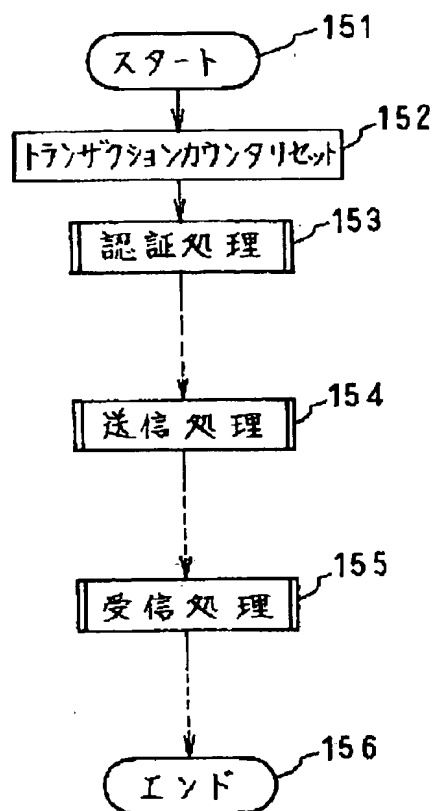
【図13】



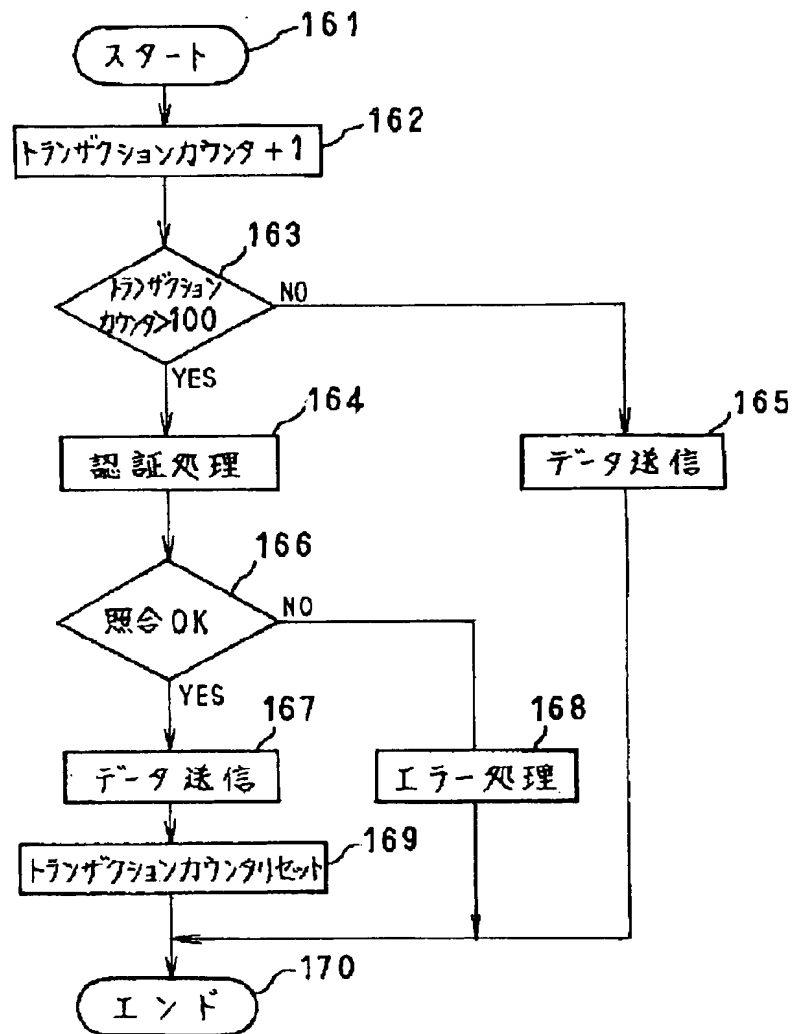
【図14】



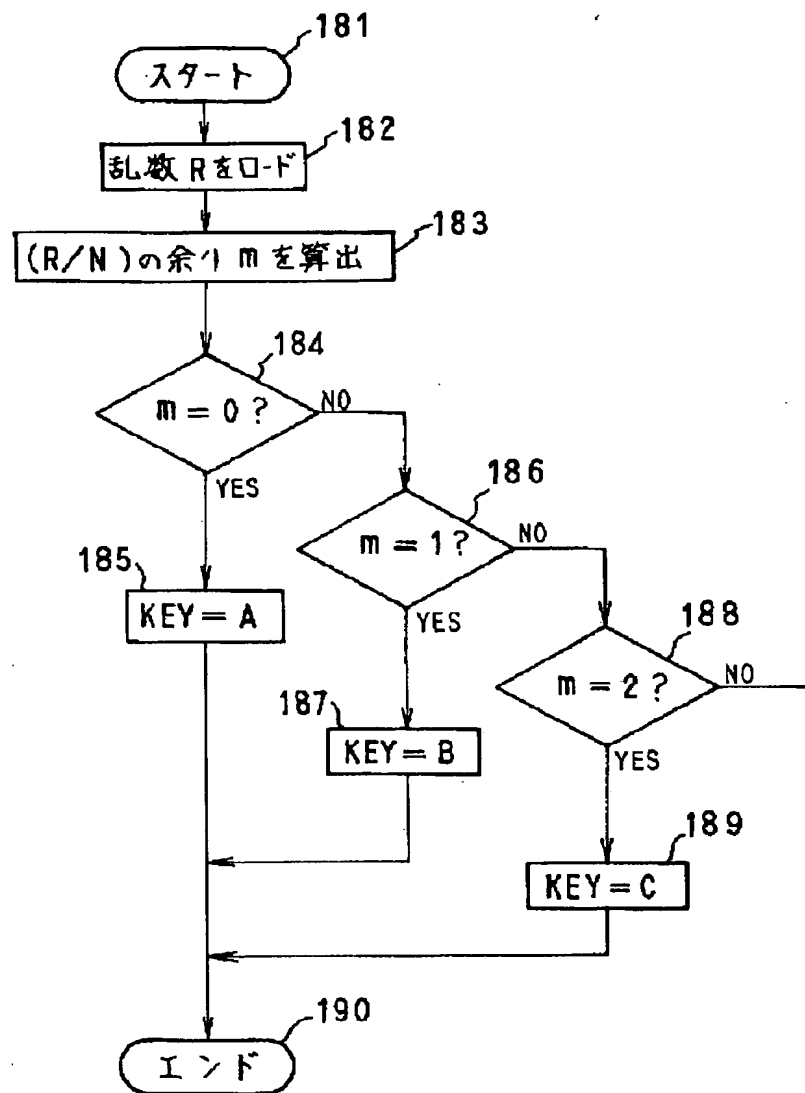
【図16】



【図17】



【図19】



【手続補正書】

【提出日】平成5年4月9日

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0031

【補正方法】変更

【補正内容】

【0031】この実施例では、ICカード13から乱数(R)を発生した後(ステップ142)、端末機27側からICカード13へ暗号化アルゴリズム($f'1$)($g'1$)を

送信する(ステップ143)。ICカード13ではRAM3の領域3-aおよび3-b、もしくはデータメモリ5の空き領域5-iおよび5-jにこれらの暗号化アルゴリズム($f'1$)($g'1$)をロードする(ステップ144)。そしてその後、上記実施例で行われている認証処理(作業)を行うようにした(ステップ145)。なお、認証処理の前に暗号化アルゴリズムを端末機側からICカード側へ送信することは、上記各実施例に適用可能である。

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.